PATENT
Attorney Docket No. 915-008.022

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In Re Application of:

Lauri PAATERO	:	Confirmation No. **7439**
Serial No: **10/804,852**	:	Examiner: **Andrew NALVEN**
Filed: **March 19, 2004**	:	Group Art Unit: **2134**

For: **PRACTICAL AND SECURE STORAGE ENCRYPTION**

Mail Stop AF
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

PRE-APPEAL BRIEF REQUEST FOR REVIEW

Sir:

In response to the final Office Action of September 8, 2008, please reconsider the rejections in view of the following remarks:

CERTIFICATE OF MAILING

I hereby certify that this paper is being deposited with the U.S. Postal Service on the date shown below with sufficient postage as first class mail in an envelope addressed to: Mail Stop AF, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

Kathleen Sipos 12/2/08
Kathleen Sipos Date

Doc Code: AP.PRE.REQ

PTO/SB/33 (07-05)
Approved for use through xx/xx/200x. OMB 0651-00xx
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

PRE-APPEAL BRIEF REQUEST FOR REVIEW

Docket Number (Optional): 915-008.022

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to "Mail Stop AF, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450" [37 CFR 1.8(a)]

on December 2, 2008

Signature: Kathleen Sipos

Typed or printed name: Kathleen Sipos

Application Number	Filed
10/804,852	March 19, 2004

First Named Inventor: Laurie PAATERO

Art Unit	Examiner
2134	Andrew NALVEN

Applicant requests review of the final rejection in the above-identified application. No amendments are being filed with this request.

This request is being filed with a notice of appeal.

The review is requested for the reason(s) stated on the attached sheet(s).
Note: No more than five (5) pages may be provided.

I am the

- ☐ applicant/inventor.
- ☐ assignee of record of the entire interest. See 37 CFR 3.71. Statement under 37 CFR 3.73(b) is enclosed. (Form PTO/SB/96)
- ☐ attorney or agent of record. Registration number _____.
- ☒ attorney or agent acting under 37 CFR 1.34. Registration number if acting under 37 CFR 1.34: 58,051

Signature

Keith R. Obert
Typed or printed name

203-261-1234
Telephone number

December 2, 2008
Date

NOTE: Signatures of all the inventors or assignees of record of the entire interest or their representative(s) are required. Submit multiple forms if more than one signature is required, see below*.

☐ *Total of _____ forms are submitted.

REMARKS

Claims 1 and 4-12 were examined by the Office, and in the final Office Action of September 8, 2008 all claims are rejected. With this response no claims are amended. Applicant respectfully submits that the Office has committed clear error in rejecting the claims for at least the following reasons. Therefore, applicant respectfully requests reconsideration and withdrawal of the rejections in view of the following discussion. This response is submitted along with a Notice of Appeal.

Claim Rejections Under § 103

In section 4, on page 3 of the Office Action, claims 1 and 4-12 are rejected under 35 U.S.C. § 103(a) as unpatentable over Grohoski (U.S. Appl. Publ. No. 2004/0225885) in view of Srinivasan et al. (U.S. Appl. Publ. No. 2004/0158742). Applicant respectfully submits that the cited references, alone or in combination, fail to disclose or suggest all of the limitations recited in claim 1. Applicant respectfully submits that the cited references at least fail to disclose or suggest that the configuration register is configured to receive mode setting instructions from a protected application.

On page 4 of the Office Action, the Office acknowledges that Grohoski fails to disclose a configuration register configured to receive mode setting instructions from a protected application, and relies upon Srinivasan for this teaching. However, Srinivasan also fails to disclose or suggest that the configuration register is configured to receive mode setting instructions from a protected application, as recited in claim 1. In contrast to claim 1, Srinivasan only discloses that in a step (216) the trusted server optionally verifies that the secure processor (110) is authorized to receive application software from the trusted server. See Srinivasan paragraph [0105]. However, Srinivasan further states that the CPU operating in secure mode receives the application software or other additional instructions from the trusted server. See Srinivasan paragraph [0107]. If the CPU is already operating in a secure mode before the application software is received from the trusted server, then the application software cannot be considered to be a protected application that provides mode setting instructions to a configuration register, as recited in claim 1.

Applicant has previously argued that Srinivasan does not disclose that the secure mode of the processor is set by a protected application. In response, the Office alleges that the application software is assured to be executed securely by the secure processor, and therefore the application software is equal to the protected application. However, as discussed in the present application, a protected application is typically a small-size application for performing security critical operations inside the secure execution environment, and is allowed to handle secret cryptographic keys. Protected applications are applications that may be issued by trusted providers, in which case they must be authenticated, but they may also be issued by any third party regardless of whether the third party is trusted or not. In the latter case, no authentication occurs.

In contrast to the present application, in Srinivasan applications corresponding to the protected applications recited in claim 1 are defined as "secure code" and "secure boot loader code." See Srinivasan paragraph [0036]. These protected applications are not the equivalent to the "application software," which the Office asserts corresponds to the protected applications recited in claim 1. Srinivasan defines "application software" as a set of instructions or parameters capable of being executed or interpreted by a processor. See Srinivasan paragraph [0031]. Since both secure code and application software are defined in the Lexicography provided in Srinivasan it implies that they are differentiated from each other. Srinivasan makes no mentioned that the application software is a protected application as mentioned in claim 1. Therefore, the section relied upon by the Office does not disclose a configuration register configured to receive mode setting instructions from a protected application, as recited in claim 1. Instead, these sections only disclose that the application software places parameters for a request for services in a set of selected registers, or performs an uncached read to a register. See Srinivasan paragraphs [0121] & [0127]. Even if the application software are considered to be a protected application, which applicant does not admit, the functions performed by the application software in Srinivasan do not correspond to providing mode setting instructions, as recited in claim 1.

Furthermore, while Srinivasan defines "secure code" and "secure boot loader code" to be interpretable or executable by the secure processor, and known to the secure processor to be trustable, the secure code and secure boot loader code do not provide mode setting instructions to

a configuration register. Claim 1 recites that the configuration register is configured to receive mode setting instructions from a protected application, however even if the secure code and secure boot loader code are considered to correspond to the protected application Srinivasan does not disclose a configuration register configured to receive mode setting instructions from the secure code or the secure boot loader code. Instead, after power on of the secure processor (110) a reset signal (A170) is asserted that indicates that the secure processor (110) has been reset. See Srinivasan paragraph [0088]. As a result, the secure mode active signal (A160) is asserted and the CPU transfers execution control to the secure boot code (A115). The secure mode active signal (A160) indicates to the non-volatile memory that the CPU is allowed to access the secure boot code, execute its instruction, and read and write data using the security information (113). See Srinivasan paragraph [0089]. However, Srinivasan does not disclose or suggest that a configuration register receives mode setting instructions from a protected application, instead it appears that the reset signal (A170) is responsible for setting the secure processor (110). Therefore, for at least these reasons claim 1 is not disclosed or suggested by the cited references.

Independent claim 12 is amended in a manner similar to claim 1, and contains limitations similar to claim 1. Therefore, for at least the reasons discussed above in relation to claim 1, claim 12 is not disclosed or suggested by the cited references.

The dependent claims depending from the above mentioned independent claims are not disclosed or suggested by the cited references at least in view of their dependencies.

Conclusion

It is therefore respectfully submitted that the present application is in condition for allowance and such action is earnestly solicited. The undersigned authorizes the Commissioner to charge any fees required to submit this response to Deposit Account No. 23-0442.

Respectfully submitted,

Dated: 2 December 2008

Keith R. Obert
Attorney for Applicant
Registration No. 58,051

WARE, FRESSOLA, VAN DER SLUYS
& ADOLPHSON LLP
Bradford Green, Building Five
755 Main Street, P.O. Box 224
Monroe, CT 06468
Telephone: (203) 261-1234
Facsimile: (203) 261-5676
USPTO Customer No. 004955